ABSTRACT OF THE DISCLOSURE

A pair of a pattern of a mask and a mask pattern obtained by bit inversion of the mask is prepared for each round function in a data scrambler. Every time encryption is to be performed, one mask pattern of the pair is randomly selected by a switch, and an exclusive OR of an input to an S-box and the selected mask pattern is calculated. In addition, an exclusive OR of an output from the S-box and bits of inverse permutation of the mask is calculated. The exclusive ORs are calculated in advance and stored as a table in the S-box. Furthermore, an exclusive OR of the output from each round function and a mask is calculated and concealed. The influence of the mask is removed by calculating the exclusive OR with the mask again on the next round.